UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,815	04/11/2005	Arvind Ramaswamy	200601202-5	6801

22879   7590   06/10/2009
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
ALI, FARHAD

ART UNIT	PAPER NUMBER
2446	

NOTIFICATION DATE	DELIVERY MODE
06/10/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
jessica.l.fusek@hp.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2009*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Status of Claims:

Claims 1-20 are pending in this Office Action.

Claims 1 and 18 are amended.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Dauerer et al. (US 5,627,967 A) in view of Noy et al. (US 6,539,540 B1).

Claim 1

Dauerer et al. teaches a data network management system for identifying

unauthorized access to a data network service **(Column 5 Lines 36-47, "Only when**

no duplicate user identifications are detected, the invention checks for invalid

user identifications. These invalid user identifications might come into existence

when an authorization has been terminated in any one of several ways"), provided

at a service node in a data network, by a user node in said data network **(Column 3**

Lines 1-4, "It is another object of the present invention to provide a control

arrangement for a file access control system which will automatically monitor and

update all lists of authorized users"), said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network **(Column 3 lines 41-45, "at least one list of the plurality of lists corresponding to each mini-disk")**, said system comprising:

a database for maintaining an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node **(Column 6 lines 14-18, "processed master list 36 and creates disk lists of users for each mini-disk contained in the master list and communicates these lists to the master file 12 where they are stored in files (e.g. L193, L198) corresponding to the associated mini-disk")**; and

a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list **(Column 7 line 55, "The new list is checked against the previous list at 306")** and for updating said authorized access list, based on the user access list retrieved from said agent **(Column 7-8 lines 66-3, "Any differences between the old and new lists detected at 306 are then categorized as to the type of change at 308 and 312. If a user ID is on the old list but not the new list, a delete command is issued at 310 to the RACF controller 18 and the master file 12, illustrated collectively as 320 in FIG. 3")**.

Dauerer et al. fails to teach a data communication means for periodically polling

said agent at said service node and for retrieving a user access list from said agent,

said user access list specifying which users have accessed said node.

However, Noy et al. teaches in Column 1 line 30, "an SNMP manager will

periodically poll an agent 30" in order to detect changes in information for a particular

network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of

invention to create the invention of Dauerer et al. to include "an SNMP manager will

periodically poll an agent 30" as taught by Noy in order to detect changes in information

for a particular network device (Column 1 lines 31-32).

Claim 2

The modified Dauerer teaches claim 1.

Dauerer et al. does not teach wherein said agent is a Simple Network

Management Protocol agent

Noy et al teaches in Column 1 lines 62-63, "receiving a first response to the

request from the SNMP agent" in order to detect changes in information for a particular

network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Dauerer et al. to include "receiving a first response to the request from the SNMP agent" as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

Claim 3

The modified Dauerer teaches claim 1.

Dauerer et al. does not teach wherein said data communication means is a Simple Network Management Protocol communication

Noy et al teaches in Column 1 lines 47-49, "The present invention seeks to provide novel methods and apparatus for optimizing Simple Network Management Protocol (SNMP) requests" in order to provide a greater efficiency than is currently known in the art. (Column 1 lines 49-50).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Dauerer et al. to include "novel methods and apparatus for optimizing Simple Network Management Protocol (SNMP) requests" as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

Claim 4

The modified Dauerer teaches claim 1.

Dauerer et al. does not teach further including means for installing said agent at said service node, said agent having means to communicate with said data communication means.

Noy et al teaches in Column 1 lines 19-20, "SNMP includes two main elements: managers and agents" in order to provide for a manager to receive information from an agent (Column 1 lines 27-29).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Dauerer et al. to include "two main elements: managers and agents" as taught by Noy in order to provide for a manager to receive information from an agent (Column 1 lines 27-29).

Claim 5

Dauerer et al. teaches a method for identifying unauthorized access to a data network service **(Column 5 Lines 36-47, "Only when no duplicate user identifications are detected, the invention checks for invalid user identifications. These invalid user identifications might come into existence when an authorization has been terminated in any one of several ways")**, provided at a service node in a data network, by a user node in said data network **(Column 3 Lines**

1-4, "It is another object of the present invention to provide a control arrangement for a file access control system which will automatically monitor and update all lists of authorized users"), said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network **(Column 3 lines 41-45, "at least one list of the plurality of lists corresponding to each mini-disk" and Column 6 lines 14-18, "processed master list 36 and creates disk lists of users for each mini-disk contained in the master list and communicates these lists to the master file 12 where they are stored in files (e.g. L193, L198) corresponding to the associated mini-disk")**, said method comprising:

> b) comparing said user access list to an authorized access list **(Column 7 line 55, "The new list is checked against the previous list at 306")**;

> c) determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list; d) if said access was not authorized, initiating a notification process; wherein said user access list identifies a plurality of accesses to said service node **(Column 5 Lines 50-67, "The manner in which invalid user identifications are found is not particularly important to the practice of the invention but could be done, for example, by comparison of access authorization or password change dates, user ID invalidation lists, etc. or a plurality of such user data items. The important fact, from a practical point of view is that any suspected invalid user ID will be reported to the authorization administrator each**

time the master list is updated and resolution of all suspected invalid

user ID's will be required before access is granted to the system.").

Dauerer et al. fails to teach a) periodically polling an agent and retrieving said

user access list, for a given period of time, from said service node in said data network.

However, Noy et al. teaches in Column 1 line 30, "an SNMP manager will

periodically poll an agent 30" in order to detect changes in information for a particular

network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of

invention to create the invention of Dauerer et al. to include "an SNMP manager will

periodically poll an agent 30" as taught by Noy in order to detect changes in information

for a particular network device (Column 1 lines 31-32).

Claim 6

The modified Dauerer et al. teaches the method as defined in claim 5, further

including updating said authorized access list based on said user access list retrieved

from said service node **(Column 7-8 lines 66-3, "Any differences between the old**

and new lists detected at 306 are then categorized as to the type of change at 308

and 312. If a user ID is on the old list but not the new list, a delete command is

issued at 310 to the RACF controller 18 and the master file 12, illustrated

collectively as 320 in FIG. 3").

Claim 7

The modified Dauerer teaches claim 5.

Dauerer et al. does not teach installing said agent at said user node, prior to periodically polling and retrieving said user access

Noy et al teaches in Column 1 lines 19-20, "SNMP includes two main elements: managers and agents" in order to provide for a manager to receive information from an agent (Column 1 lines 27-29).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Dauerer et al. to include "two main elements: managers and agents" as taught by Noy in order to provide for a manager to receive information from an agent (Column 1 lines 27-29).

Claim 8

The modified Dauerer et al. teaches the method as defined in claim 5, further including selecting said service node for identification based on a predetermined criteria, prior to retrieving said user access list **(Column 8 Lines 31-38, "Once the authorization administrator has edited the master list 26 and issued an immediate change command at 322, a check is made to determine if the disk lists involved**

are available and, as before, branches to end 326 under the error condition of the

unavailability of the lists. If the appropriate lists are available, the disk lists are

updated beginning at step 302, as described above").

Claim 9

The modified Dauerer et al. teaches the method as defined in claim 5, wherein

said notification process comprises notifying a Network Operations Console **(Column 5**

Lines 50-67, "The important fact, from a practical point of view is that any

suspected invalid user ID will be reported to the authorization administrator each

time the master list is updated and resolution of all suspected invalid user ID's

will be required before access is granted to the system").

Claim 10

The modified Dauerer et al. teaches the method as defined in claim 5, wherein a)

through c) are repeated, and wherein said user node is selected from one of a plurality

of user nodes in said data network **(Column 5 lines 2-15, "Access to the system to**

update mini-disk access lists and an existing processed master list 36, reflecting

the mini-disk access lists, to correspond to an updated master list 26 can be

deferred until such time as access by a user is actually required. For instance, the

updating of the master list within the system can be carried out on a regular

schedule when user traffic is low and thus avoid conflicts with needs for the

system by users").

Claim 11

The modified Dauerer et al. teaches the method as defined in claim 5, wherein a)

through d) are repeated, and wherein said user node is selected from one of a plurality

of user nodes in said data network **(Column 5 lines 2-15, "Access to the system to**

update mini-disk access lists and an existing processed master list 36, reflecting

the mini-disk access lists, to correspond to an updated master list 26 can be

deferred until such time as access by a user is actually required. For instance, the

updating of the master list within the system can be carried out on a regular

schedule when user traffic is low and thus avoid conflicts with needs for the

system by users").

Claim 12

The modified Dauerer teaches claim 5.

Dauerer et al. does not teach wherein said agent is a Simple Network

Management Protocol agent

Noy et al teaches in Column 1 lines 62-63, "receiving a first response to the request from the SNMP agent" in order to detect changes in information for a particular network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Dauerer et al. to include "receiving a first response to the request from the SNMP agent" as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

Claim 13

Dauerer et al. teaches a computer-readable medium for identifying unauthorized access to a data network service **(Column 5 Lines 36-47, "Only when no duplicate user identifications are detected, the invention checks for invalid user identifications. These invalid user identifications might come into existence when an authorization has been terminated in any one of several ways")**, provided at a service node in a data network, by a user node in said data network **(Column 3 Lines 1-4, "It is another object of the present invention to provide a control arrangement for a file access control system which will automatically monitor and update all lists of authorized users")**, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network **(Column 3 lines 41-45, "at least one list of the plurality of lists corresponding to each mini-disk"**

and Column 6 lines 14-18, "processed master list 36 and creates disk lists of

users for each mini-disk contained in the master list and communicates these

lists to the master file 12 where they are stored in files (e.g. L193, L198)

corresponding to the associated mini-disk"), and said medium having stored

thereon, computer-readable and computer-executable instructions which, when

executed by a processor, cause said processor to perform steps comprising:

> b) comparing said user access list to an authorized access list **(Column 7 line**
>
>   **55, "The new list is checked against the previous list at 306");**

> c) determining if an access to said data network service was authorized based on
>
>   said comparison step b);   d) if determined that said access was unauthorized,
>
>   initiating a notification process **(Column 5 Lines 50-67, "The manner in**
>
>   **which invalid user identifications are found is not particularly important**
>
>   **to the practice of the invention but could be done, for example, by**
>
>   **comparison of access authorization or password change dates, user ID**
>
>   **invalidation lists, etc. or a plurality of such user data items. The**
>
>   **important fact, from a practical point of view is that any suspected invalid**
>
>   **user ID will be reported to the authorization administrator each time the**
>
>   **master list is updated and resolution of all suspected invalid user ID's**
>
>   **will be required before access is granted to the system.").**

Dauerer et al. fails to teach a) periodically polling an agent and retrieving said

user access list, for a given period of time, from said service node in said data network.

However, Noy et al. teaches in Column 1 line 30, "an SNMP manager will periodically poll an agent 30" in order to detect changes in information for a particular network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Dauerer et al. to include "an SNMP manager will periodically poll an agent 30" as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

Claim 14

The modified Dauerer et al. teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of updating said authorized access list based on user access information **(Column 7-8 lines 66-3, "Any differences between the old and new lists detected at 306 are then categorized as to the type of change at 308 and 312. If a user ID is on the old list but not the new list, a delete command is issued at 310 to the RACF controller 18 and the master file 12, illustrated collectively as 320 in FIG. 3")**.

Claim 15

The modified Dauerer teaches claim 13.

Dauerer et al. does not teach further containing computer-readable and computer-executable instructions which perform a step of installing said agent at said user node, prior to retrieving said user access list in step a).

Noy et al teaches in Column 1 lines 19-20, "SNMP includes two main elements: managers and agents" in order to provide for a manager to receive information from an agent (Column 1 lines 27-29).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Dauerer et al. to include "two main elements: managers and agents" as taught by Noy in order to provide for a manager to receive information from an agent (Column 1 lines 27-29).

Claim 16

The modified Dauerer et al. teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions wherein said steps a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network **(Column 5 lines 2-15, "Access to the system to update mini-disk access lists and an existing processed master list 36, reflecting the mini-disk access lists, to correspond to an updated master list 26 can be deferred until such time as access by a user is actually required. For instance, the updating of the master list within the system can be**

carried out on a regular schedule when user traffic is low and thus avoid conflicts

with needs for the system by users").

Claim 17

The modified Dauerer teaches claim 13.

Dauerer et al. does not teach wherein said agent is a Simple Network

Management Protocol agent

Noy et al teaches in Column 1 lines 62-63, "receiving a first response to the

request from the SNMP agent" in order to detect changes in information for a particular

network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of

invention to create the invention of Dauerer et al. to include "receiving a first response to

the request from the SNMP agent" as taught by Noy in order to detect changes in

information for a particular network device (Column 1 lines 31-32).

Claim 18

Dauerer et al. teaches a computer for use in a data network for identifying

unauthorized access to a data network service **(Column 5 Lines 36-47, "Only when**

no duplicate user identifications are detected, the invention checks for invalid

user identifications. These invalid user identifications might come into existence

when an authorization has been terminated in any one of several ways"), provided

at a service node in a data network, by a user node in said data network **(Column 3**

Lines 1-4, "It is another object of the present invention to provide a control

arrangement for a file access control system which will automatically monitor and

update all lists of authorized users"), said service node having an agent and having

means for maintaining a user access list, said user access list having at least one data

network address corresponding to at least one user node in said data network, said

computer comprising: means for storing an authorized access list for said service node,

said authorized access list specifying which users are authorized to access said service

node **(Column 3 lines 41-45, "at least one list of the plurality of lists**

corresponding to each mini-disk" and Column 6 lines 14-18, "processed master

list 36 and creates disk lists of users for each mini-disk contained in the master

list and communicates these lists to the master file 12 where they are stored in

files (e.g. L193, L198) corresponding to the associated mini-disk");

a central processing unit **(See Figure 1 #14, "CPU")**.

data processing means for comparing said retrieved user access list to said

authorized access list **(Column 7 line 55, "The new list is checked against**

the previous list at 306") and for updating said authorized access list based

on the user access list retrieved from said agent **(Column 7-8 lines 66-3,**

"Any differences between the old and new lists detected at 306 are then

categorized as to the type of change at 308 and 312. If a user ID is on the

old list but not the new list, a delete command is issued at 310 to the

RACF controller 18 and the master file 12, illustrated collectively as 320

in FIG. 3").

Dauerer et al. fails to teach a data communication means for periodically polling

said agent at said service node and for retrieving a user access list from said agent,

said user access list specifying which users are authorized to access said service node.

However, Noy et al. teaches in Column 1 line 30, "an SNMP manager will

periodically poll an agent 30" in order to detect changes in information for a particular

network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of

invention to create the invention of Dauerer et al. to include "an SNMP manager will

periodically poll an agent 30" as taught by Noy in order to detect changes in information

for a particular network device (Column 1 lines 31-32).

Claim 19

The modified Dauerer et al. teaches the data network as defined in claim 1,

wherein said authorized access list is a common authorized user access list, that

includes a range of user nodes for comparing to said user access list to determine if

said user access list is a subset of said common authorization access list **(Column 3**

lines 41-45, "at least one list of the plurality of lists corresponding to each mini-

disk" and Column 6 lines 14-18, "processed master list 36 and creates disk lists

of users for each mini-disk contained in the master list and communicates these

lists to the master file 12 where they are stored in files (e.g. L193, L198)

corresponding to the associated mini-disk").

Claim 20

The modified Dauerer Dauerer et al. teaches the data network management

system of claim 1 wherein said user access list identifies a plurality of accesses to said

service node **(Column 3 Lines 1-4, "It is another object of the present invention to**

provide a control arrangement for a file access control system which will

automatically monitor and update all lists of authorized users" and See Fig. 4A).

Response to Arguments

3.   Applicant's arguments filed 02/06/2009 have been fully considered but they are

not persuasive.

In regards to the applicants arguments that Dauerer does not teach or even

suggest that the Network node contains a user access list of users that have accessed

the node, and that this is compared to the authorized access list, the examiner

respectfully disagrees. Dauerer teaches in Column 5-6 lines 36-9, "Only when no

duplicate user identifications are detected, the invention checks for invalid user

identifications. These invalid user identifications might come into existence when an

authorization has been terminated in any one of several ways. If a user identification is

to be invalidated but not properly carried out, the user ID could be carried in the system

for extended periods of time, possibly months or years, and presents a substantial

security risk. The manner in which invalid user identifications are found is not

particularly important to the practice of the invention but could be done, for example, by

comparison of access authorization or password change dates, user ID invalidation

lists, etc. or a plurality of such user data items. The important fact, from a practical point

of view is that any suspected invalid user ID will be reported to the authorization

administrator each time the master list is updated and resolution of all suspected invalid

user ID's will be required before access is granted to the system. In a preferred form of

the invention, however, a transaction is individually carried out against all user ID's in

master list 26. Specifically, it is desired to remove invalid user ID's from the master list

which could, for example, occur when a user ID is invalidated by some transaction in

the system which is not reported to the system administrator and, hence, not reflected in

a deletion from the master list 26. Therefore, any invalid user ID which has not been

removed from the master list may still be listed in the RACF list of authorized users for a

mini-disk. In this case, if a new user ID were to be issued that had the same name as

the previously deleted user ID, it would, undesirably, have the same mini-disk access as

the previous user. Thus, the preferred form of the invention determines if any user ID's

in the master list 26 are invalidated or otherwise not present in the system as reflected

in processed master list 36." Clearly Dauerer has a means for checking for invalid user

identifications wherein a list specifying which users have accessed said service node is

read upon by comparison of access authorization or password change dates, user ID

invalidation lists, etc. or a plurality of such user data items.

In regards to an agent, Noy is relied upon for the teaching of periodic polling, and

furthermore the examiner asserts that an agent is well known in the art and is even

described in the applicants description of the prior art which is herein considered as

applicants admitted prior art, see applicants specification paragraph [0006] "The model

assumed by SNMP is a central management station and a number of data collection

points, known to the skilled artisan as software agents, or simply as agents. The agents

are instructed by the management station as to what information to collect. The

management stations then collect this information from the agents through SNMP. The

data and functions that the agent supports are specified in a well known data structure

called a Management Information Base (MIB). The MIB specifies which variables the

management station contains, such as the information that can be queried and set by

the management station".

Conclusion

4.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FARHAD ALI whose telephone number is (571)270-1920. The examiner can normally be reached on Monday thru Friday, 7:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Farhad Ali/
Examiner, Art Unit 2446

/Jeffrey Pwu/
Supervisory Patent Examiner, Art Unit 2446